A global estimation of the lower bound of the privacy amplification term for decoy-state quantum key distribution

Haodong Jiang, Ming Gao,* Hong Wang, Hongxin Li, and Zhi Ma†
State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, Henan, China
(Dated: February 17, 2015)

The privacy amplification term, of which the lower bound needs to be estimated with the decoy-state method, plays a positive role in the secure key rate formula for decoy-state quantum key distribution. In previous work, the yield and the bit error rate of single-photon state are estimated separately to gain this lower bound. In this work, we for the first time take the privacy amplification term as a whole to consider this lower bound. The mathematical description for the correlation between the yield and the bit error rate of single-photon state is given with just two unknown variables. Based on this, we obtain the global estimation of this lower bound for both BB84 protocol and measurement-device-independent protocol. The results of numerical simulation show that the global estimation can significantly improve the performance of quantum key distribution.

PACS numbers: 03.67.Dd, 42.81.Gs, 03.67.Hk

I. INTRODUCTION

Quantum key distribution (QKD) based on the laws of quantum physics can theoretically present an unconditionally secure communication [1–3]. However, there is a gap between its theory and practice due to the imperfection in real-life implementation. Particularly, the eavesdropper (Eve) can launch attacks aiming at the imperfect single-photon source and the limited detector efficiency in practical QKD system [4–9]. By utilizing the decoy-state method [10–12], the practical QKD setups with an imperfect single-photon source can be still secure.

To deal with the threat coming from the detectors [13], several approaches have been proposed. One is device-independent QKD (DI-QKD) [14] of which the security is based on the violation of a Bell inequality. However, DI-QKD con not apply to existing practical system because a loophole-free Bell test at the moment is still unavailable. Another one is measurement-device-independent quantum key distribution (MDI-QKD) [15, 16] based on the idea of entanglement swapping which can remove all detector side channel attacks.

The security of BB84 protocol with imperfect devices is analyzed in [17–21]. The security of MDI-QKD protocol is researched in [16, 22, 23]. Some useful formulas are given to calculate the secure key rate for practical BB84 protocol and MDI-QKD protocol. The privacy amplification term makes a positive contribution in these secure key rate formulas and it can not be measured in the experiment. In asymptotic case, the yield of single-photon state is basis independent [24–26]. Then the privacy amplification term can be calculated in just one basis.

In previous work [27], the lower bound of this term is obtained by estimating the lower bound of the yield Y_1 of single-photon state and the upper bound of the bit error rate e_1 of single-photon state separately. The lower bound of the yield Y_1 is estimated from the gain equations while the upper bound of the bit error rate e_1 is estimated from the quantum bit error rate (QBER) equations. The yield Y_i of i-photon state existing in both the gain equations and the QBER equations is the link between the estimation of lower bound of Y_1 and that of upper bound of e_1. When Y_i is one certain value, the minimum of Y_1 is reached. But the maximum of e_1 may be reached as Y_i is another certain value. That is to say, the lower bound of Y_1 and the upper bound of e_1 may not be simultaneously reached. Thus, the separate estimation can just bring a lower bound of the privacy amplification term instead of the minimum.

Inspired by Wang's method [12, 25, 28, 29], we give a mathematical description of the correlation between Y_1 and e_1 with just two unknown variables. In particular, we will show that globally estimating the lower bound of the privacy amplification term is equal to finding the minimum of a bivariate continuous function in a closed area. Thus the minimum of the privacy amplification term can be attained with the global estimation and higher secure key rate can be achieved.

The article is organized as follows. Section II introduces the global estimation of the lower bound of the privacy amplification term for BB84 protocol. The global estimation for MDI-QKD protocol will be discussed in section III. We conclude our work in section IV.

II. THE GLOBAL ESTIMATION OF THE LOWER BOUND OF THE PRIVACY AMPLIFICATION TERM FOR BB84 PROTOCOL

The privacy amplification term for BB84 protocol is given by $Y_1[1-H(e_1)]$, where Y_1 and e_1 are, respectively, the yield and the bit error rate of single-photon state. Here in this section, firstly we mathematically characterize the correlation between Y_1 and e_1. Then the minimum of $Y_1[1-H(e_1)]$ is given with the method of global estimation. Lastly, the numerical simulation is performed

* gaoming.zhengzhou@gmail.com
† ma_zhi@163.com

to make a comparison in performance of QKD protocol between the global estimation and the separated estimation.

A. The correlation between Y_1 and e_1

Given a weak coherent state source which sends three different kinds of optical pulses with intensities ω, υ and μ ($0 = \omega < \upsilon < \mu$), the overall gains which mean the probability for Bob to obtain a detection event in one pulse are given by following three equations,

$$Q_\mu = \sum_{i=0}^{\infty} e^{-\mu} \frac{\mu^i}{i!} Y_i, \tag{1}$$

$$Q_\upsilon = \sum_{i=0}^{\infty} e^{-\upsilon} \frac{\upsilon^i}{i!} Y_i, \tag{2}$$

$$Q_\omega = Y_0, \tag{3}$$

where Q_ν and Y_i are, respectively, the overall gain with intensity ν ($\nu \in \{\omega, \upsilon, \mu\}$) and the yield of i-photon state.

We denote E_ν to be the overall QBER with intensity ν, e_i to be the bit error rate of i-photon state. The overall QBER equations can be given by

$$E_\mu Q_\mu = \sum_{i=0}^{\infty} e^{-\mu} \frac{\mu^i}{i!} e_i Y_i, \tag{4}$$

$$E_\upsilon Q_\upsilon = \sum_{i=0}^{\infty} e^{-\upsilon} \frac{\upsilon^i}{i!} e_i Y_i, \tag{5}$$

$$E_\omega Q_\omega = e_0 Y_0. \tag{6}$$

It is important to note that Y_0 is equal to the gain Q_ω when Alice does not send any optical pulse, which includes the detector dark count and other background contributions. As the background is random, we assume that $E_\omega = e_0 = 0.5$.

As three equations can only fix three variables, we temporarily take Y_i ($i \geq 3$) as known variables. Then three gain equations can be solved according to Cramer's rule. Y_1 is given by

$$Y_1 = \frac{\mu}{\upsilon(\mu-\upsilon)}(e^\upsilon Q_\upsilon - Y_0) - \frac{\upsilon}{\mu(\mu-\upsilon)}(e^\mu Q_\mu - Y_0) + \sum_{i=3}^{\infty} \frac{(\mu^{i-1}\upsilon - \upsilon^{i-1}\mu)}{i!(\mu-\upsilon)} Y_i. \tag{7}$$

Similarly, $e_1 Y_1$ can be gained by

$$e_1 Y_1 = \frac{\mu}{\upsilon(\mu-\upsilon)}(e^\upsilon E_\upsilon Q_\upsilon - e_0 Y_0) - \frac{\upsilon}{\mu(\mu-\upsilon)} (e^\mu E_\mu Q_\mu - e_0 Y_0) + \sum_{i=3}^{\infty} \frac{(\mu^{i-1}\upsilon - \upsilon^{i-1}\mu)}{i!(\mu-\upsilon)} e_i Y_i. \tag{8}$$

From equation (7) and equation(8), we can get that there are infinite variables Y_i ($i \geq 3$) simultaneously influencing the values of Y_1 and $e_1 Y_1$. Then the privacy amplification term is influenced by infinite variables. It is computationally infeasible to find the minimum of a function with infinite variables. Fortunately, we find a way to reduce the number of unknown variables to two inspired by Wang's method [12, 25]. We define a state of which the density operator is $\rho = \sum_{i=3}^{\infty} \frac{(\mu^{i-1}\upsilon - \upsilon^{i-1}\mu)}{\Omega i!(\mu-\upsilon)} |i\rangle \langle i|$ ($\Omega = \sum_{i=3}^{\infty} \frac{(\mu^{i-1}\upsilon - \upsilon^{i-1}\mu)}{i!(\mu-\upsilon)} > 0$). The yield and the bit error rate of this state can be given by

$$Y_\rho = \sum_{i=3}^{\infty} \frac{(\mu^{i-1}\upsilon - \upsilon^{i-1}\mu)}{i!(\mu-\upsilon)\Omega} Y_i, \tag{9}$$

$$e_\rho Y_\rho = \sum_{i=3}^{\infty} \frac{(\mu^{i-1}\upsilon - \upsilon^{i-1}\mu)}{i!(\mu-\upsilon)\Omega} e_i Y_i. \tag{10}$$

Then equation (7) and equation (8) can be rewritten as

$$Y_1 = \frac{\mu}{\upsilon(\mu-\upsilon)}(e^\upsilon Q_\upsilon - Y_0) - \frac{\upsilon}{\mu(\mu-\upsilon)}(e^\mu Q_\mu - Y_0) + \Omega Y_\rho, \tag{11}$$

$$e_1 Y_1 = \frac{\mu}{\upsilon(\mu-\upsilon)}(e^\upsilon E_\upsilon Q_\upsilon - e_0 Y_0) - \frac{\upsilon}{\mu(\mu-\upsilon)} (e^\mu E_\mu Q_\mu - e_0 Y_0) + \Omega e_\rho Y_\rho. \tag{12}$$

Thus Y_1 and $e_1 Y_1$ is determined by the gains and the QBERs which can be measured in the experiment except the yield and the bit error rate of state ρ. State ρ is the link between the calculations of Y_1 and $e_1 Y_1$. The yield Y_ρ of state ρ as a unknown variable simultaneously influences the estimations of both Y_1 and e_1. In [30], Y_ρ is set to 0 to get the lower bound of Y_1 while e_ρ and Y_ρ are both set to 1 to get the upper bound of e_1. Thus the contradiction that Y_ρ cannot be simultaneously 0 and 1 emerges.

The quantity of the privacy amplification term is $Y_1[1 - H(e_1)]$, which is a bivariate continuous function of Y_ρ and e_ρ. The minimum of the continuous function on the closed area can be attained. This is one reason why we should consider the global lower bound of $Y_1[1-H(e_1)]$ instead of calculating the lower bound of Y_1 and the upper bound of e_1 separately. In previous work [11, 12, 30, 31], the lower bound of Y_1 is gained by utilizing the gain equations. In fact, Y_1 also exists in QBER equations where the information of Y_1 is not extracted. This is another motivation that the global lower bound of $Y_1[1 - H(e_1)]$ should be considered.

B. The global lower bound of $Y_1[1-H(e_1)]$

According to previous work [11, 12, 30, 31], the most accurate estimations of Y_1 and e_1 are given by

$$Y_1 \geq Y_1^L = \frac{\mu}{\upsilon(\mu-\upsilon)}(e^{\upsilon}Q_{\upsilon} - Y_0) - \frac{\upsilon}{\mu(\mu-\upsilon)}(e^{\mu}Q_{\mu} - Y_0), \quad (13)$$

$$e_1 \leq e_1^U = \frac{(e^{\upsilon}E_{\upsilon}Q_{\upsilon} - e_0Y_0)}{\upsilon Y_1^L}. \quad (14)$$

According to the corollary in appendix, the global lower bound of $Y_1[1-H(e_1)]$ can be gained by

$$Y_1(1-H(e_1)) \geq (Y_1^L+\theta)[1-H(\frac{e_1^U Y_1^L}{Y_1^L+\theta})],$$
$$\theta = \frac{1}{\mu(\mu-\upsilon)}[\upsilon(e^{\mu}E_{\mu}Q_{\mu} - e_0Y_0) - \mu(e^{\upsilon}E_{\upsilon}Q_{\upsilon} - e_0Y_0)] > 0. \quad (15)$$

To make a clear comparison, we denote (Y_1^G, e_1^G) as the point where the minimum is achieved. Corresponding to equation (13) and equation (14), Y_1^G and e_1^G are given by

$$Y_1^G = Y_1^L + \theta, \quad (16)$$

$$e_1^G = \frac{e_1^U Y_1^L}{Y_1^L+\theta}. \quad (17)$$

Here θ can be considered the information of Y_1 coming from the QBER equations, which is abandoned for the separate estimation. By globally considering the lower bound of the privacy amplification term, we successfully extract it.

C. Numerical simulation for BB84 protocol

With the observed gains and error rates, the final secure key rate can be calculated [17] by

$$R \geq p_1^{\mu}Y_1[1-H(e_1)] - Q_{\mu}fH(E_{\mu}), \quad (18)$$

where p_1^{μ} is the probability that Alice sends a single-photon state pulse corresponding to signal state μ; f is the error correction inefficiency; $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. For a fair comparison, we use the same parameters in [28, 29] summarized in table I. For simplicity, the detection efficiency is put to the overall channel transmission, hence we only need to assume the 100% detection efficiency at Bob's side.

The ratios of the estimations of Y_1 with two methods (equation (13) and equation (16)) to the asymptotic limit calculated with the infinite-intensity decoy-state method are shown in figure 1. The ratios of the asymptotic limit of e_1 to the estimations with two methods (equation (14) and equation (17)) are shown in figure 2. The ratios of the secure key rates computed with two methods (separate estimation and global estimation) to the asymptotic limit are shown in figure 3. From the results, we can see tighter estimations of Y_1 and e_1 are gained with the method of global estimation. Thus, higher secure key rates are achieved.

TABLE I. List of parameters for numerical simulation

e_0	f	p_d	e_d
0.5	1.16	3×10^{-6}	1.5%

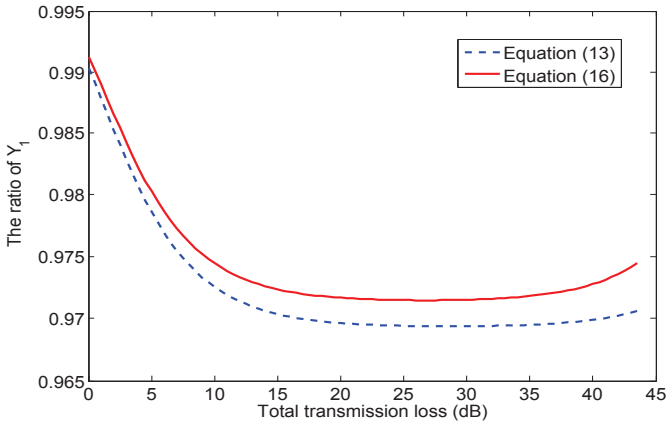

FIG. 1. (Color online) The ratio of the estimation of Y_1 to the asymptotic limit calculated with the infinite-intensity decoy-state method vs the total channel transmission loss for three-intensity decoy-state BB84 protocol. We set $\upsilon = 0.1$, $\mu = 0.5$ for decoy state and signal state, respectively.

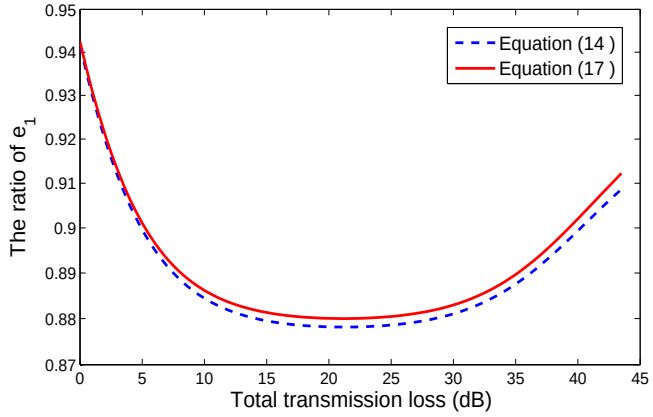

FIG. 2. (Color online) The ratio of the asymptotic limit calculated with the infinite-intensity decoy-state method to the estimation of e_1 vs the total channel transmission loss for three-intensity decoy-state BB84 protocol. We set $\upsilon = 0.1$, $\mu = 0.5$ for decoy state and signal state, respectively.

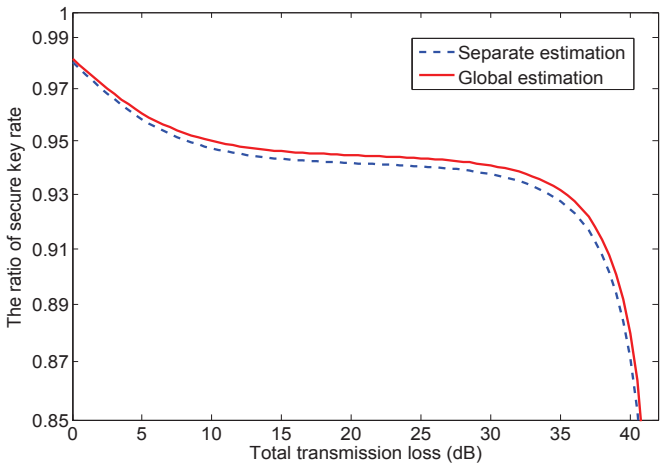

FIG. 3. (Color online) The ratio of the secure key rate calculated with the three-intensity decoy-state method to the asymptotic limit calculated with the infinite-intensity decoy-state method vs the total channel transmission loss for decoy-state BB84 protocol. We set $\upsilon = 0.1$, $\mu = 0.5$ for decoy state and signal state, respectively.

III. THE GLOBAL ESTIMATION OF THE LOWER BOUND OF THE PRIVACY AMPLIFICATION TERM FOR MDI-QKD PROTOCOL

For MDI-QKD protocol, the secure key rate is gained [16] by

$$R \geq p_{11}^z Y_{11}^z [1 - H(e_{11}^x)] - Q_{\mu_a\mu_b}^z f H(E_{\mu_a\mu_b}^z), \quad (19)$$

where p_{11}^z is the probability that Alice and Bob simultaneously send single-photon state pulses corresponding to signal state in z basis; $Q_{\mu_a\mu_b}^z$ and $E_{\mu_a\mu_b}^z$ are the gain and QBER when Alice and Bob simultaneously send signal state pulses; Y_{11}^z and e_{11}^x are the yield in Z basis and the bit error rate in X basis when Alice and Bob simultaneously send single-photon state pulses.

The variable values in (19) can be measured in the experiment except Y_{11}^z and e_{11}^x. So the major task in the calculation of secure key rate is estimating the lower bound of $Y_{11}^z[1 - H(e_{11}^x)]$. In previous work, to get the lower bound of $Y_{11}^z[1 - H(e_{11}^x)]$, the lower bound of Y_{11}^z and the upper bound of e_{11}^x are calculated separately.

In fact, Y_{11}^z is equal to Y_{11}^x in asymptotic setting according to [25]. As a result, we will not temporarily distinguish the basis of Y_{11} and e_{11}. We will consider the lower bound of $Y_{11}[1 - H(e_{11})]$ as a whole.

Similarly, in this section we will firstly introduce the mathematical description of the correlation between Y_{11} and e_{11}. Then the global lower bound of $Y_{11}[1 - H(e_{11})]$ is calculated. Lastly, the results of numerical simulation will be given. The following work is on basis of the three-intensity decoy-state MDI-QKD protocol [28].

A. The correlation between Y_{11} and e_{11}

For MDI-QKD protocol, the gain and QBER when Alice (Bob) sends a certain pulse with intensity q_a (q_b) can be given by

$$Q_{q_a q_b} = \sum_{i,j=0}^{\infty} e^{-(q_a+q_b)} \frac{{q_a}^i {q_b}^j}{i!j!} Y_{ij}, \quad (20)$$

$$E_{q_a q_b} Q_{q_a q_b} = \sum_{i,j=0}^{\infty} e^{-(q_a+q_b)} \frac{{q_a}^i {q_b}^j}{i!j!} e_{ij} Y_{ij}, \quad (21)$$

where Y_{ij} and e_{ij} is the yield and the bit error rate when Alice (Bob) sends an i-photon (j-photon) state pulse.

Given two weak coherent state sources which send three different kinds of optical pulses with intensities $(0 = \omega_a < \upsilon_a < \mu_a)$ and $(0 = \omega_b < \upsilon_b < \mu_b)$, we eliminate the unknown variables Y_{0i} and Y_{j0}, then get

$$e^{(\mu_a+\mu_b)} \tilde{Q}_{\mu_a\mu_b} = \sum_{i,j=1}^{\infty} \frac{\mu_a^i \mu_b^j}{i!j!} Y_{ij}, \quad (22)$$

$$e^{(\mu_a+\upsilon_b)} \tilde{Q}_{\mu_a\upsilon_b} = \sum_{i,j=1}^{\infty} \frac{\mu_a^i \upsilon_b^j}{i!j!} Y_{ij}, \quad (23)$$

$$e^{(\upsilon_a+\mu_b)} \tilde{Q}_{\upsilon_a\mu_b} = \sum_{i,j=1}^{\infty} \frac{\upsilon_a^i \mu_b^j}{i!j!} Y_{ij}, \quad (24)$$

$$e^{(\upsilon_a+\upsilon_b)} \tilde{Q}_{\upsilon_a\upsilon_b} = \sum_{i,j=1}^{\infty} \frac{\upsilon_a^i \upsilon_b^j}{i!j!} Y_{ij}, \quad (25)$$

where $\tilde{Q}_{\mu_1,\mu_2}(\mu_1 \in \{\mu_a, \upsilon_a\}, \mu_2 \in \{\mu_b, \upsilon_b\})$ is achieved by

$$\begin{aligned} \tilde{Q}_{\mu_1\mu_2} =& Q_{\mu_1\mu_2} + e^{-(\mu_1+\mu_2)} Q_{\omega_a\omega_b} \\ & - e^{-\mu_1} Q_{\omega_a\mu_2} - e^{-\mu_2} Q_{\mu_1\omega_b}. \end{aligned} \quad (26)$$

According to [28], Y_{11} can be solved from equations (23, 24 and 25),

$$Y_{1,1} = Y_{11}^L + \sum_{(i+j)\geq 4} \frac{\Upsilon_{i,j} Y_{i,j}}{i!j!(\mu_a - \upsilon_a)(\mu_b - \upsilon_b)}, \quad (27)$$

$$\begin{aligned} &\Upsilon_{i,j} = \upsilon_a^{i-1}\mu_b^{j-1}\upsilon_b(\mu_a - \upsilon_a) + \mu_a^{i-1}\upsilon_b^{j-1}\upsilon_a(\mu_b - \upsilon_b) \\ &-\upsilon_a^{i-1}\upsilon_b^{j-1}(\mu_a\mu_b - \upsilon_a\upsilon_b) > 0, \\ &Y_{11}^L = \frac{1}{(\mu_a - \upsilon_a)(\mu_b - \upsilon_b)} \Big(\frac{e^{(\upsilon_a+\upsilon_b)}(\mu_a\mu_b - \upsilon_a\upsilon_b)}{\upsilon_a\upsilon_b} \tilde{Q}_{\upsilon_a\upsilon_b} - \\ &\frac{e^{(\mu_a+\upsilon_b)}\upsilon_a(\mu_b - \upsilon_b)}{\mu_a\upsilon_b} \tilde{Q}_{\mu_a\upsilon_b} - \frac{e^{(\upsilon_a+\mu_b)}\upsilon_b(\mu_a - \upsilon_a)}{\upsilon_a\mu_b} \tilde{Q}_{\upsilon_a\mu_b} \Big). \end{aligned} \quad (28)$$

Similarly, e_{11} can be solved from the corresponding

QBER equations,

$$e_{11}Y_{11} = (e_{11}Y_{11})^L + \sum_{(i+j)\geq 4} \frac{e_{i,j}\Upsilon_{i,j}Y_{i,j}}{i!j!(\mu_a-\upsilon_a)(\mu_b-\upsilon_b)}, \quad (29)$$

$$(e_{11}Y_{11})^L = \frac{1}{(\mu_a-\upsilon_a)(\mu_b-\upsilon_b)}\left(\frac{e^{(\upsilon_a+\upsilon_b)}(\mu_a\mu_b-\upsilon_a\upsilon_b)}{\upsilon_a\upsilon_b}\right.$$
$$\tilde{Q}_{\upsilon_a\upsilon_b}\tilde{E}_{\upsilon_a\upsilon_b} - \frac{e^{(\mu_a+\upsilon_b)}\upsilon_a(\mu_b-\upsilon_b)}{\mu_a\upsilon_b}\tilde{E}_{\mu_a\upsilon_b}\tilde{Q}_{\mu_a\upsilon_b} -$$
$$\left.\frac{e^{(\upsilon_a+\mu_b)}\upsilon_b(\mu_a-\upsilon_a)}{\upsilon_a\mu_b}\tilde{E}_{\upsilon_a\mu_b}\tilde{Q}_{\upsilon_a\mu_b}\right). \quad (30)$$

$\tilde{E}_{\mu_1,\mu_2}\tilde{Q}_{\mu_1,\mu_2}(\mu_1 \in \{\mu_a,\upsilon_a\}, \mu_2 \in \{\mu_b,\upsilon_b\})$ is achieved by

$$\tilde{E}_{\mu_1\mu_2}\tilde{Q}_{\mu_1\mu_2} = E_{\mu_1\mu_2}Q_{\mu_1\mu_2} + e^{-(\mu_1+\mu_2)}E_{\omega_a\omega_b}Q_{\omega_a\omega_b} - e^{-\mu_1}E_{\omega_a\mu_2}Q_{\omega_a\mu_2} - e^{-\mu_2}E_{\mu_1\omega_b}Q_{\mu_1\omega_b}. \quad (31)$$

It is easy to verify that $\Upsilon_{i,j}$ is positive when $(i+j) \geq 4$. So we can define a state of which the density operator is $\psi = \sum_{(i+j)\geq 4} \frac{\Upsilon_{i,j}}{i!j!(\mu_a-\upsilon_a)(\mu_b-\upsilon_b)\Pi}(|i\rangle\langle i| \otimes |j\rangle\langle j|)$, where Π is equal to $\sum_{(i+j)\geq 4} \frac{\Upsilon_{i,j}}{i!j!(\mu_a-\upsilon_a)(\mu_b-\upsilon_b)}$.

Then equation (27) and equation (29) can be rewritten

$$Y_{11} = Y_{11}^L + \Pi Y_\psi, \quad (32)$$
$$e_{11}Y_{11} = (e_{11}Y_{11}^L)^L + \Pi e_\psi Y_\psi, \quad (33)$$

where Y_ψ and e_ψ is the yield and the bit error rate of state ψ.

Thus Y_{11} and e_{11} is linked by the state ψ. $Y_{11}(1-H(e_{11}))$ is a bivariate continuous function with two parameter variables Y_ψ and e_ψ. The lower bound of Y_{11} can be gained by setting Y_ψ to 0 while the upper bound of e_{11} can be gained by setting Y_ψ and e_ψ to 1. Thus the lower bound of $Y_{11}(1-H(e_{11}))$ can not be reached with the separate estimation. The minimum of $Y_{11}(1-H(e_{11}))$ can be attained with the global estimation.

B. The global lower bound of $Y_{11}(1-H(e_{11}))$

In [28], the lower bound of Y_{11} is given in equation (28) by setting the last term in equation (27) to 0. The upper bound of e_{11} is given by setting the term $e_{ij}Y_{ij}$ $(i+j) \geq 2$ of $\tilde{E}_{\upsilon_a\upsilon_b}\tilde{Q}_{\upsilon_a\upsilon_b}$ to 0,

$$e_{11} \leq e_{11}^U = \frac{e^{\upsilon_a+\upsilon_b}\tilde{E}_{\upsilon_a\upsilon_b}\tilde{Q}_{\upsilon_a\upsilon_b}}{\upsilon_a\upsilon_b Y_{11}^L}. \quad (34)$$

According equations (32, 33 and 34) and corollary in appendix, the global lower bound of $Y_{11}(1-H[e_{11}])$ is given by

$$Y_{11}[1-H(e_{11})] \geq (Y_{11}^L+\delta)[1-H(\frac{e_{11}^U Y_{11}^L}{Y_{11}^L+\delta})], \quad (35)$$
$$\delta = e_{11}^U Y_{11}^L - (e_{11}Y_{11})^L > 0.$$

To make a clear comparison, we denote (Y_{11}^G, e_{11}^G) as the point where the minimum is attained. Corresponding to equation (28) and equation (34), Y_{11}^G and e_{11}^G is given by

$$Y_{11}^G = Y_{11}^L + \delta, \quad (36)$$
$$e_{11}^G = \frac{e_{11}^U Y_{11}^L}{Y_{11}^L+\delta}. \quad (37)$$

C. Numerical simulation for MDI-QKD protocol

Numerical simulations are performed with the parameters in table I. The ratios of the estimations of Y_{11} with two methods (equation (28) and equation (36)) to the asymptotic limit obtained with the infinite-intensity decoy-state method are shown in figure 4. The ratios of the asymptotic limit of e_{11} to the estimations with two methods (equation (34) and equation (37)) are shown in figure 5. The ratios of the secure key rates calculated with two methods (separate estimation and global estimation) to the asymptotic limit are shown in figure 6. From the results, we can see tighter estimations of Y_{11} and e_{11} are gained with global estimation. Thus, higher secure key rates are reached.

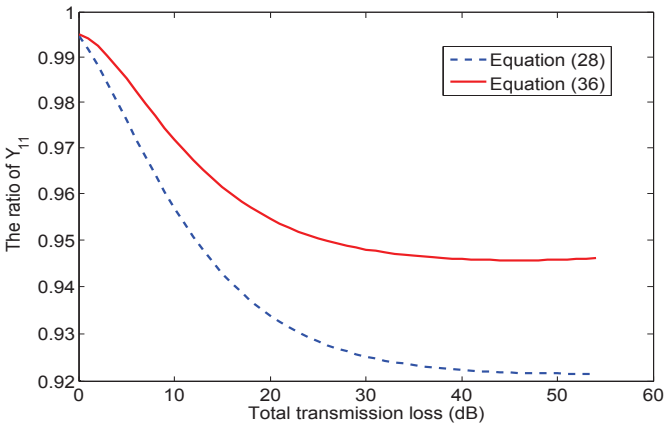

FIG. 4. (Color online) The ratio of the estimation of Y_{11} to the asymptotic limit calculated with the infinite-intensity decoy-state method vs the total channel transmission loss for three-intensity decoy-state MDI-QKD protocol. We set $\upsilon_a = \upsilon_b = 0.1$, $\mu_a = \mu_b = 0.5$ for decoy states and signal states, respectively.

IV. CONCLUSION

The global estimations of the privacy amplification term for both BB84 protocol and MDI-QKD protocol have been researched in this paper. Conventional separate estimation will abandon the information of the yield of single-photon state in QBER equations. With the global estimation of the privacy amplification term, this information has been extracted and the minimum of the

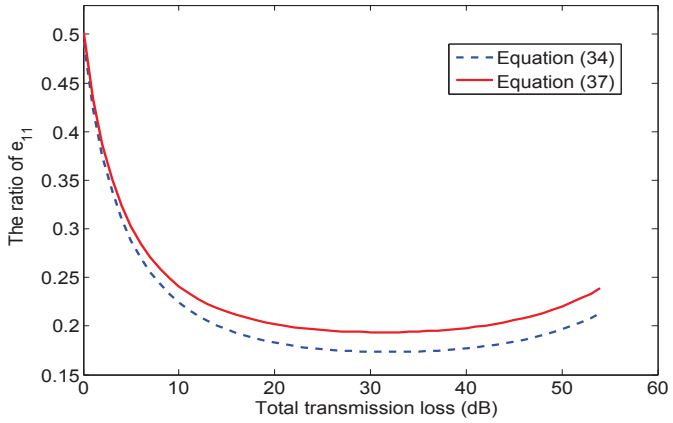

FIG. 5. (Color online) The ratio of the asymptotic limit of e_{11} calculated with the infinite-intensity decoy-state method to the estimation vs the total channel transmission loss for three-intensity decoy-state MDI-QKD protocol. We set $\upsilon_a = \upsilon_b = 0.1$, $\mu_a = \mu_b = 0.5$ for decoy states and signal states, respectively.

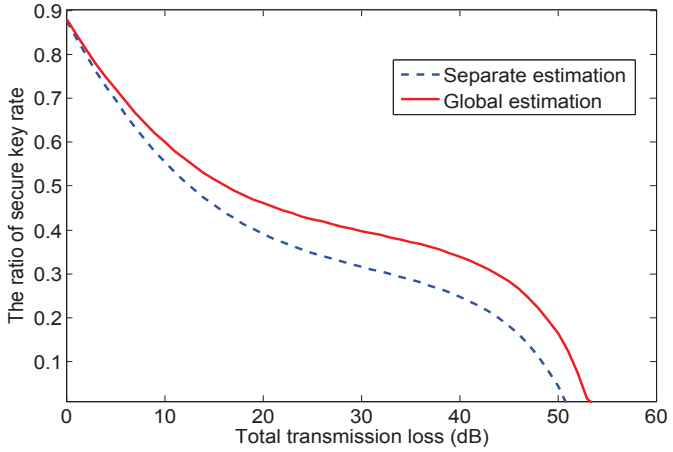

FIG. 6. (Color online) The ratio of secure key rate calculated with the three-intensity decoy-state method to the asymptotic limit calculated with the infinite-intensity decoy-state method vs the total channel transmission loss for decoy-state MDI-QKD protocol. We set $\upsilon_a = \upsilon_b = 0.1$, $\mu_a = \mu_b = 0.5$ for decoy states and signal states, respectively.

privacy amplification term is achieved. Compared with separate consideration, more accurate estimations of the yield and the bit error rate of single-photon state are gained, which thus significantly improve the performance of the quantum key distribution for both BB84 protocol and MDI-QKD protocol. Additionally, more accurate separate estimation will contribute to more smaller domain of the bivariate function which thus can further help to obtain a tighter global estimation.

APPENDIX

Theorem: For the bivariate continuous function $f(x,y) = (A+Cy)[1-H(\frac{B+Cxy}{A+Cy})]$ $(A>0, C>0)$ with the definition domain $\{(x,y): 0\le x\le 1, 0\le y\le 1, \frac{B+Cxy}{A+Cy} < 0.5\}$, the minimum can be attained on the border.

proof: Firstly, the partial derivatives of function $f(x,y)$ are given by

$$f_x = -(A+Cy)H(\frac{B+Cxy}{(A+Cy)})'\frac{Cy}{A+Cy}, \tag{38}$$

$$\begin{aligned} f_y =& C[1-H(\frac{B+Cxy}{A+Cy})] - (A+Cy)H(\frac{B+Cxy}{A+Cy})' \\ & \frac{(ACx-BC)}{(A+Cy)^2}. \end{aligned} \tag{39}$$

If there is an extreme point (x_0, y_0) $(0<x_0<1, 0<y_0<1)$, then $H(\frac{B+Cxy}{A+Cy})'$ has to be 0 from the restrict $f_x = 0$. Combine the restrict $f_y = 0$, we can get $C[1-H(\frac{B+Cxy}{A+Cy})] = 0$. This is in contradiction with our initial assumption.

Function $f(x,y)$ for a fixed y is a decreasing function with parameter variable x. So the minimum can be reached where x is 1. So this problem is converted to searching the minimum of univariate continuous function $g(y) = (A+y)[1-H(\frac{B+y}{A+y})](0\le y\le C)$. Calculating the derivative function of $g(y)$, we can find

$$\begin{aligned} g_y =& 1-H(\frac{B+y}{A+y}) - (A+y)H(\frac{B+y}{A+y})'\frac{(A-B)}{(A+y)^2} \\ =& 1+(\frac{B+y}{A+y})\log(\frac{B+y}{A+y}) + (\frac{A-B}{A+y})\log(\frac{A-B}{A+y}) \\ & -(\frac{A-B}{A+y})\log(\frac{A-B}{B+y}) \\ =& 1+\log(\frac{B+y}{A+y}). \end{aligned} \tag{40}$$

As we assume $\frac{B+y}{A+y} < 1/2$, then $g_y < 0$. That is to say, g_y is a decreasing function with parameter variable y.

Corollary: For the bivariate continuous function $f(x,y) = (A+Cy)[1-H(\frac{B+Cxy}{A+Cy})]$ $(A>0, C>0)$ with the definition domain $\{(x,y): 0\le x\le 1, 0\le y\le 1, \frac{B+Cxy}{A+Cy} < 0.5, (B+Cxy) < D, (A+Cy) > E\}$, the nonzero minimum can be obtained in the following three cases.

case 1: when $(D-B) < C$ and $(D-B) > (E-A)$, the minimum is $f(1, \frac{D-B}{C}) = (A+D-B)[1-H(\frac{D}{A+D-B})]$.

case 2: when $(D-B) < C$ and $(D-B) < (E-A)$, the minimum is $f(\frac{D-B}{E-A}, \frac{E-A}{C}) = E[1-H(\frac{D}{E})]$.

case 3: when $(D-B) >= C$, the minimum is $f(1,1) = (A+C)[1-H(\frac{B+C}{A+C})]$.

proof: If we set $(B+Cxy) = D$, the function $f(x,y)$ is converted to an univariate continuous increasing function $(A+Cy)[1-H(\frac{D}{A+Cy})]$. Then it is easy to verify

the correctness of corollary combining with the proof of theorem.

ACKNOWLEDGEMENTS

This work is supported by the National High Technology Research and Development Program of China Grant No.2011AA010803, the National Natural Science Foundation of China Grants No.61472446 and No.U1204602 and the Open Project Program of the State Key Laboratory of Mathematical Engineering and Advanced Computing Grant No.2013A14.

[1] Charles H Bennett, Gilles Brassard, et al. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175. New York, 1984.

[2] Dominic Mayers. Unconditional security in quantum cryptography. *Journal of the ACM (JACM)*, 48(3):351–406, 2001.

[3] Artur K Ekert. Quantum cryptography based on bells theorem. *Physical review letters*, 67(6):661, 1991.

[4] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C Sanders. Limitations on practical quantum cryptography. *Physical Review Letters*, 85(6):1330, 2000.

[5] Norbert Lütkenhaus and Mika Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4(1):44, 2002.

[6] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Physical Review A*, 78(4):042333, 2008.

[7] Feihu Xu, Bing Qi, and Hoi-Kwong Lo. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New Journal of Physics*, 12(11):113026, 2010.

[8] Henning Weier, Harald Krauss, Markus Rau, Martin Fuerst, Sebastian Nauerth, and Harald Weinfurter. Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New Journal of Physics*, 13(7):073024, 2011.

[9] Nitin Jain, Christoffer Wittmann, Lars Lydersen, Carlos Wiechers, Dominique Elser, Christoph Marquardt, Vadim Makarov, and Gerd Leuchs. Device calibration impacts security of quantum key distribution. *Physical Review Letters*, 107(11):110501, 2011.

[10] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters*, 91(5):057901, 2003.

[11] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94(23):230504, 2005.

[12] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical review letters*, 94(23):230503, 2005.

[13] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature photonics*, 4(10):686–689, 2010.

[14] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

[15] Samuel L Braunstein and Stefano Pirandola. Side-channel-free quantum key distribution. *Physical review letters*, 108(13):130502, 2012.

[16] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical review letters*, 108(13):130503, 2012.

[17] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, page 136. IEEE.

[18] Hitoshi Inamori, Norbert Lütkenhaus, and Dominic Mayers. Unconditional security of practical quantum key distribution. *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, 41(3):599–627, 2007.

[19] Valerio Scarani and Renato Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Physical review letters*, 100(20):200501, 2008.

[20] Raymond YQ Cai and Valerio Scarani. Finite-key analysis for practical implementations of quantum key distribution. *New Journal of Physics*, 11(4):045024, 2009.

[21] Charles Ci Wen Lim, Marcos Curty, Nino Walenta, Feihu Xu, and Hugo Zbinden. Concise security bounds for practical decoy-state quantum key distribution. *Physical Review A*, 89(2):022307, 2014.

[22] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature communications*, 3:634, 2012.

[23] Marcos Curty, Feihu Xu, Wei Cui, Charles Ci Wen Lim, Kiyoshi Tamaki, and Hoi-Kwong Lo. Finite-key analysis for measurement-device-independent quantum key distribution. *Nature communications*, 5, 2014.

[24] Zhengchao Wei, Weilong Wang, Zhen Zhang, Ming Gao, Zhi Ma, and Xiongfeng Ma. Decoy-state quantum key distribution with biased basis choice. *Scientific reports*, 3, 2013.

[25] Xiang-Bin Wang. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Physical Review A*, 87(1):012320, 2013.

[26] Zong-Wen Yu, Yi-Heng Zhou, and Xiang-bin Wang. Decoy state method for measurement device independent quantum key distribution with different intensities in only one basis. *arXiv preprint arXiv:1309.0471*, 2013.

[27] For simplicity, the analysis in Sec. I is for BB84 protocol. The same analysis for MDI-QKD protocol is presented in Sec. III.

[28] Zong-Wen Yu, Yi-Heng Zhou, and Xiang-Bin Wang. Three-intensity decoy-state method for measurement-device-independent quantum key distribution. *Physical Review A*, 88(6):062339, 2013.

[29] Yi-Heng Zhou, Zong-Wen Yu, and Xiang-Bin Wang. Tightened estimation can improve the key rate of measurement-device-independent quantum key distribution by more than 100%. *Physical Review A*, 89(5):052325, 2014.

[30] Masahito Hayashi. General theory for decoy-state quantum key distribution with an arbitrary number of intensities. *New Journal of Physics*, 9(8):284, 2007.

[31] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Physical Review A*, 72(1):012326, 2005.